Europ. J. Combinatorics (1991) **12,** 477–482

Maximal Sets of Mutually Orthogonal Latin Squares. I

ANTHONY B. EVANS

One problem of interest in the study of latin squares is that of determining parameter pairs (n, r) for which there exists a maximal set of r mutually orthogonal latin squares of order n. In this paper we find new such parameter pairs by constructing maximal sets of mutually orthogonal latin squares using difference matrices. In the process we generalize known non-existence results for complete mappings, strong complete mappings and Knut Vic designs.

INTRODUCTION

Let G be an abelian group of order n, written additively with identity 0, and let $D = \{d_{ij}\}$ be an $r \times \lambda n$ matrix with entries from G. Then we call D an $(n, r; \lambda, G)$ difference matrix if for each $i, j, i \neq j$; the sequence $\{d_{jk} - d_{ik}: k = 1, \ldots, \lambda n\}$ contains each element of G exactly λ times. D is a maximal difference matrix if there exists no $(n, r+1; \lambda, G)$ difference matrix $D' = \{d'_{ij}\}$ satisfying $d'_{ij} = d_{ij}$ for $i = 1, \ldots, r$ and $j = 1, \ldots, \lambda n$. For D an $r \times n$ matrix, we shall use mD to denote the $r \times mn$ matrix $(D \cdots D)$, consisting of m consecutive copies of D. Thus if D is an $(n, r; \lambda, G)$ difference matrix then mD will be an $(n, r; m\lambda, G)$ difference matrix.

Hall and Paige [6] proved that a finite group the Sylow 2-subgroup of which is non-trivial and cyclic cannot admit a complete mapping. This result was subsequently generalized by Drake [4]. Evans [5] proved that a finite group the Sylow 3-subgroup of which is non-trivial and cyclic cannot admit a strong complete mapping if there exists a homomorphism from the group onto its Sylow 3-subgroup. Each of these proofs relies on establishing the maximality of difference matrices the entries of which are elements of cyclic groups of prime power order. This suggests that these results might be special cases of a more general theorem on maximal difference matrices. In this paper we construct maximal $(mp^r, p; 1, G)$ difference matrices, where p is a prime, r a positive integer, and m a positive integer relatively prime to p. This will generalize the above-mentioned results of Hall and Paige, Drake, and Evans. This will also yield constructions of new maximal sets of mutually orthogonal latin squares.

A *latin square* of order n is an $n \times n$ matrix with entries from a symbol set of order n, such that each symbol appears exactly once in each row and column. Two latin squares, on the same symbol set, are said to be *orthogonal* if upon superimposing the squares each ordered pair of symbols appears exactly once. A set of pairwise orthogonal latin squares is called a *mutually orthogonal* set of latin squares. We shall say that a set of mutually orthogonal latin squares is *maximal* if there exists no latin square orthogonal to each square of the set. For more information on maximal sets of mutually orthogonal latin squares, see Beth, Jungnickel, and Lenz [1, ch. X]. Ostrom [10] proved implicitly that the existence of a maximal $(n, r; 1, G)$ difference matrix implied the existence of a maximal set of $r - 1$ mutually orthogonal latin squares of order n. For which parameter pairs (n, r) do there exist maximal sets of r mutually orthogonal latin squares of order n? We will show that if p is a prime and r is a positive integer then there exists a maximal set of $p - 1$ mutually orthogonal latin squares of order p^r. Special cases of this result have been proved before. The case $r = 1$ is well known, the case $p = 2$ has been proved many times, and the case $p = 3$, $r = 2$ was

0195-6698/91/060477 + 06 $02.00/0 © 1991 Academic Press Limited

proved by Jungnickel and Grams [9] using a computer search. We will also show that whenever p is a prime, m is not divisible by p, and there exist $p-1$ mutually orthogonal latin squares of order m, then there exists a maximal set of $p-1$ mutually orthogonal latin squares of order mp^r, for any positive integer r.

The Construction

The first result that we need is proved implicitly in Ostrom [10], and provides our justification for the study of maximal difference matrices.

Lemma 1 (Ostrom). *If there exists of a maximal $(n, r; 1, G)$ difference matrix then there exists a maximal set of $r-1$ mutually orthogonal latin squares of order n.*

Proof. See Beth, Jungnickel, and Lenz [1, p. 540, Theorem 12.8]. □

We next derive a similar result for certain $(n, r; m, G)$ difference matrices. These two results will be essential for our constructions of maximal sets of mutually orthogonal latin squares.

Theorem 1. *Let D be an $(n, r; 1, G)$ difference matrix for which mD is maximal. If there exist $r-1$ mutually orthogonal latin squares of order m then there exists a maximal set of $r-1$ mutually orthogonal latin squares of order nm.*

Proof. If D' is obtained from D by permuting rows and columns, or by adding a constant to all the elements of any row or column of D, then D' will still be a difference matrix and mD' will still be maximal. Thus we are free to assume that $D=(d_{ij})$, $d_{1j}=0$ for all j. Let $L_k=(a_{ij}^k)$, $k=1,\ldots,r-1$, be a set of mutually orthogonal latin squares of order m, on the symbol set $\{0,\ldots,m-1\}$. Define $\mathscr{L}_k=(b_{ij}^k)$ by $b_{ij}^k=d_{2i}+d_{k+1\,j}$. Then $\mathscr{L}_1,\ldots,\mathscr{L}_{r-1}$ is a set of mutually orthogonal latin squares of order n.

Form the Kronecker products $L_1\times\mathscr{L}_1,\ldots,L_{r-1}\times\mathscr{L}_{r-1}$. This is a set of mutually orthogonal latin squares of order mn with entries from the symbol set $\{(i,g): g\in G, i=0,\ldots,m-1\}$. Suppose that there exists a latin square M orthogonal to each of $L_1\times\mathscr{L}_1,\ldots,L_{r-1}\times\mathscr{L}_{r-1}$. The symbol $(0,0)$ will occur exactly once as an entry in each row and column of M. Let the corresponding cells of $L_1\times\mathscr{L}_1$ contain $(a_{i_sj_s}^1, b_{u_sv_s}^1)$, $s=1,\ldots,mn$. Define an $(r+1)\times mn$ matrix $D'=(d'_{ij})$, $d'_{1s}=0$ for $s=1,\ldots,mn$, $d'_{k+1\,s}=d_{k+1\,v_s}$ for $s=1,\ldots,mn$ and $k=1,\ldots,r-1$, and $d'_{r+1\,s}=-d_{2u_s}$ for $s=1,\ldots,mn$. The sequence $\{d_{r+1\,j}-d_{1j}: j=1,\ldots,mn\}=\{-d_{2u_s}: s=1,\ldots,mn\}$ contains each element of G exactly m times as the sequence $\{u_s: s=1,\ldots,mn\}$ contains m copies of each integer $i=1,\ldots,n$. The sequence $\{d_{r+1\,j}-d_{k+1\,j}: j=1,\ldots,mn\}=\{-(d_{2u_s}+d_{k+1\,v_s}): s=1,\ldots,mn\}=(-b_{u_sv_s}^k: s=1,\ldots,mn\}$ contains each element of G exactly m times as each element of the symbol set occurs exactly once in the sequence $\{(a_{i_sj_s}^k, b_{u_sv_s}^k): s=1,\ldots,mn\}$. Thus D' is an $(n, r+1; m, G)$ difference matrix. This contradicts the maximality of mD. □

The conclusion of Theorem 1 also holds true for non-abelian groups, although we will be restricting ourselves to cyclic groups in this paper. Thus we are led to ask for which $(n, r; 1, G)$ difference matrices D and which positive integers m is mD a maximal difference matrix? Obvious necessary conditions are that D be maximal and that n not divide m. These are not sufficient, however, as if $G=Z_n$, n even, and D is any $(n, 2; 1, G)$ difference matrix then D will be maximal, but mD will be maximal iff m is odd. We will give constructions of maximal difference matrices of the form mD.

Drake [3] proved that if n does not divide m then the existence of a projective plane of order n and the existence of $n-1$ mutually orthogonal latin squares of order m implies the existence of a maximal set of $n-1$ mutually orthogonal latin squares of order mn. A straightforward modification of Drake's proof yields the following result.

THEOREM 2. *If D is an $(n, n; 1, G)$ difference matrix then mD is maximal iff n does not divide m.*

This theorem also holds true for non-abelian groups, although the only groups for which such difference matrices are known to exist are the elementary abelian groups. Theorem 2 cannot yield any new parameter pairs for maximal sets of mutually orthogonal latin squares, but it does give rise to difference matrix proofs of some known results. Corollaries 1 and 2 follow immediately from Theorems 1 and 2.

COROLLARY 1 (Drake [3]). *If q is a prime power, q does not divide m, and there exist $q-1$ mutually orthogonal latin squares of order m, then there exists a maximal set of $q-1$ mutually orthogonal latin squares of order qm.*

COROLLARY 2 (Bruck [2]). *If q is the smallest prime power that divides n then there exists a maximal set of $q-1$ mutually orthogonal latin squares of order n.*

We next determine some new parameter pairs for maximal sets of mutually orthogonal latin squares. We will construct, for p a prime, maximal sets of $p-1$ mutually orthogonal latin squares of order p^r, and maximal sets of $p-1$ mutually orthogonal latin squares of order mp^r, for certain values of m. First we need two lemmas.

LEMMA 2. *Let $n=p^r$, p a prime, and let $\phi\colon \{0, \ldots, p-1\} \to \{0, \ldots, n-1\}$ be any function satisfying $\phi(i) \equiv i$ modulo p, and let $d_1, \ldots, d_{p-1}$ be integers. Then the system of equations $\sum_{i=1}^{p-1} x_i \phi(i)^j \equiv d_j$ modulo n, $j=1, \ldots, p-1$, has a unique solution modulo n.*

PROOF. For $r=1$ this is known to be true. Suppose this to be true for $r=k$ and consider the case $r=k+1$. Set $x_i = y_i + z_i p^k$, where $0 \leqslant y_i < p^k$ and $0 \leqslant z_i < p$. $\sum_{i=1}^{p-1} x_i \phi(i)^j \equiv \sum_{i=1}^{p-1} y_i \phi(i)^j + (\sum_{i=1}^{p-1} z_i \phi(i)^j) p^k \equiv d_j$ modulo n. Modulo p^k the y_is are uniquely determined. $\sum_{i=1}^{p-1} y_i \phi(i)^j \equiv c_j$ modulo n and $c_j \equiv d_j$ modulo p^k.

Thus $(\sum_{i=1}^{p-1} z_i \phi(i)^j) p^k \equiv d_j - c_j$ modulo n or $\sum_{i=1}^{p-1} z_i \phi(i)^j \equiv (d_j - c_j)/p^k$ modulo p. Thus the z_is are also uniquely determined. Hence the result. □

LEMMA 3. *If n is a power of a prime p then $\sum_{i=0}^{n-1} i^{p-1} \equiv (n/p)(p-1)$ modulo n.*

PROOF. We know this formula to be correct if n is a prime or $p=2$, so let us assume that $n=p^r$, p an odd prime, $r>1$, and that we have proved the formula correct for all smaller powers of p. Let g be primitive modulo n. Then

$$\sum_{i=0}^{n-1} i^{p-1} \equiv \sum_{j=1}^{n-(n/p)} (g^j)^{p-1} + \sum_{j=0}^{(n/p)-1} (jp)^{p-1}$$

$$\equiv \sum_{j=1}^{n-(n/p)} g^{j(p-1)} + p^{p-1} \sum_{j=0}^{(n/p)-1} j^{p-1} \text{ modulo } n.$$

If $r=2$ then $p^{p-1}\equiv 0$ modulo n. If $r>2$ then, by the inductive hypothesis, $\sum_{j=0}^{(n/p)-1} j^{p-1}\equiv 0$ modulo n/p^2 and so $p^{p-1}\sum_{j=0}^{(n/p)-1} j^{p-1}\equiv 0$ modulo n.

Thus $\sum_{i=0}^{n-1} i^{p-1}\equiv \sum_{j=1}^{n-(n/p)} g^{j(p-1)}\equiv (p-1)\sum_{k=0}^{(n/p)-1}(kp+1)\equiv (p-1)\sum_{k=0}^{(n/p)-1} kp + (p-1)(n/p)\equiv (p-1)(n/p)$ modulo n. □

THEOREM 3. *Let G be the group Z_n, $n=p^r$, p a prime, let $\phi\colon\{0,\ldots,p-1\}\to\{0,\ldots,n-1\}$ be any function satisfying $\phi(i)\equiv i$ modulo p, and suppose that p does not divide m. Let D be the $(n,p;1,G)$—difference matrix with ij th entry $\phi(i-1)j$ modulo n, $i=1,\ldots,p$, $j=0,\ldots,n-1$. Then mD is a maximal difference matrix.*

PROOF. Let d_{ij} denote the ij th entry of mD, $i=1,\ldots,p$ and $j=1,\ldots,mn$, and suppose that mD is not maximal. Then we may add an extra row, the entry of which in the j th column is d_j, $j=1,\ldots,mn$.

By Lemma 2, we may choose $a_1,\ldots,a_{p-1}$ to satisfy

$$\sum_{i=1}^{p-1} a_i\phi(i)^j\equiv\begin{cases}0 \text{ modulo } n & \text{for } j<p-1,\\ 1 \text{ modulo } n & \text{for } j=p-1.\end{cases}$$

Then

$$\begin{aligned}
m(a_1+\cdots+a_{p-1})\sum_{x=0}^{n-1} x^{p-1} &\equiv \sum_{i=2}^{p} a_{i-1}\sum_{j=1}^{mn}(d_j-d_{ij})^{p-1}\\
&\equiv \sum_{i=2}^{p} a_{i-1}\sum_{j=1}^{mn}(d_j-\phi(i-1)d_{2j}/\phi(1))^{p-1}\\
&\equiv \sum_{j=1}^{mn}\Bigg(\sum_{k=0}^{p-1}\binom{p-1}{k}(-1)^{p-1-k}d_j^k(d_{2j}/\phi(1))^{p-1-k}\\
&\quad\times\sum_{i=2}^{p} a_{i-1}\phi(i-1)^{p-1-k}\Bigg)\\
&\equiv \sum_{j=1}^{mn} d_j^{p-1}\sum_{i=2}^{p} a_{i-1}+(-1)^{p-1}\sum_{j=1}^{mn}(d_{2j}/\phi(1))^{p-1}\\
&\equiv m(a_1+\cdots+a_{p-1}+\varepsilon)\sum_{x=0}^{n-1} x^{p-1} \text{ modulo } n,
\end{aligned}$$

where $\varepsilon=1$ if $p>2$, -1 if $p=2$. Therefore $m\sum_{x=0}^{n-1} x^{p-1}\equiv 0$ modulo n, contradicting Lemma 3. Hence the result. □

In the following corollaries we list several applications of Theorem 3. From this theorem we are able to derive known non-existence results for complete mappings, strong complete mappings and Knut Vic designs, as well as some new constructions of maximal sets of mutually orthogonal latin squares.

A *complete mapping* of a group G is a bijection $\theta\colon G\to G$ for which the mapping $x\to x\theta(x)$ is also a bijection.

COROLLARY 3 (Hall and Paige [6]). *A finite group G with a non-trivial, cyclic Sylow 2-subgroup does not admit complete mappings.*

PROOF. Let $g_1,\ldots,g_{mn}$ be the elements of G and let n be the order of the Sylow 2-subgroup of G. Then there exists a homomorphism $\psi\colon G\to Z_n$. Suppose that G admits a complete mapping θ. Then the $3\times nm$ matrix $D'=(d_{ij})$, $d_{1j}=0$, $d_{2j}\equiv\psi(j)^{-1}$

modulo n, $d_{3j} \equiv \psi\theta(j)$ modulo n is an $(n, 3; m, Z_n)$ difference matrix. But this contradicts the maximality of the $(n, 2; m, Z_n)$ difference matrix $D = (c_{ij})$, $c_{ij} = d_{ij}$ for all i, j. □

This same argument can be generalized.

COROLLARY 4 (Drake [4]). *If G is a finite group with a non-trivial, cyclic Sylow 2-subgroup and λ is odd then any $(|G|, 2; \lambda, G)$ difference matrix is maximal.*

PROOF. In the proof of Corollary 3 construct $\lambda D'$ instead of D'. □

A *strong complete mapping* of a group G is a complete mapping θ of G for which the mapping $x \to x^{-1}\theta(x)$ is a bijection.

COROLLARY 5 (Evans [5]). *A finite group the Sylow 3-subgroup of which is non-trivial and cyclic cannot admit a strong complete mapping if there exists a homomorphism from the group onto its Sylow 3-subgroup.*

PROOF. Let $g_1, \ldots, g_{mn}$ be the elements of G and let n be the order of the Sylow 3-subgroup of G. There exists a homomorphism $\psi: G \to Z_n$. Suppose that G admits a strong complete mapping θ. Then the $4 \times nm$ matrix $D' = (d_{ij})$, $d_{1j} = 0$, $d_{2j} \equiv \psi(j)$ modulo n, $d_{3j} \equiv \psi(j)^{-1}$ modulo n, $d_{4j} \equiv \psi\theta(j)$ modulo n, is an $(n, 4; m, Z_n)$ difference matrix. But this contradicts the maximality of the $(n, 3; m, Z_n)$ difference matrix $D = (c_{ij})$, $c_{ij} = d_{ij}$ for all i, j. □

A *Knut Vic design* of order n is a latin square of order n in which each symbol appears exactly once on each (broken) left and right diagonal. It was proved in Evans [5] that a Knut Vic design of order n exists iff the cyclic group Z_n admits a strong complete mapping.

COROLLARY 6 (Hedayat [7] and Hedayat and Federer [8]). *There exists a Knut Vic design of order $n > 1$ iff n is not divisible by 2 or 3.*

PROOF. The non-existence of such designs follows from Corollaries 3 and 5, and the existence from the observation that, if n is not divisible by 2 or 3 then the mapping $x \to 2x$ is a strong complete mapping of Z_n. □

The last two corollaries describe the implications of Theorem 3 for the existence of maximal sets of mutually orthogonal latin squares.

COROLLARY 7. *Let $n = p^r$, p a prime and $r \geq 1$. Then there exists a maximal set of $p - 1$ mutually orthogonal latin squares of order n.*

PROOF. By Lemma 1, if there exists a maximal $(n, r; 1, G)$ difference matrix then there exists a maximal set of $r - 1$ mutually orthogonal latin squares of order n. □

COROLLARY 8. *Let $n = p^r m$, p a prime, $r \geq 1$, and p and m relatively prime. If there exist $p - 1$ mutually orthogonal latin squares of order m then there exists a maximal set of $p - 1$ mutually orthogonal latin squares of order n.*

PROOF. This is an immediate consequence of Theorems 1 and 3. □

We list some special cases of Corollaries 7 and 8.

EXAMPLES. (1) If $n = m2^s$, m odd, then there exists a latin square of order n that has no orthogonal mate. This was first proved by Euler in 1779 and has since been rediscovered several times.

(2) If $n = m3^s$, m not divisible by 3, then there exists a maximal set of 2 mutually orthogonal latin squares of order n whenever $m \neq 2$. The special case $m = 1$, $s = 2$, can be found in Jungnickel and Grams [9], where it is proved using a computer search.

(3) If $n = m5^s$, m not divisible by 5, then there exists a maximal set of 4 mutually orthogonal latin squares of order n whenever $m > 52$.

(4) More generally, if $n = mp^s$, m not divisible by p, p a prime, then there exists a maximal set of $p - 1$ mutually orthogonal latin squares of order n whenever m is sufficiently large.

REFERENCES

1. T. Beth, D. Jungnickel and H. Lenz, *Design Theory*, Wissenschaftsverlag, Mannheim, 1984.
2. R. H. Bruck, Finite nets. I; numerical invariants, *Can. J. Math.*, **3** (1951), 94–107.
3. D. A. Drake, Maximal sets of Latin squares and partial transversals, *J. Statist. Plann. Inf.*, **1** (1977), 143–149.
4. D. A. Drake, Partial λ-geometries and generalized Hadamard matrices over groups, *Can. J. Math.*, **31**(3) (1979), 617–627.
5. A. B. Evans, On strong complete mappings, *Congr. Numer.* **70** (1991) 241–248.
6. M. Hall and L. J. Paige, Complete mappings of finite groups, *Pac. J. Math.*, **5** (1955), 541–549.
7. A. Hedayat, A complete solution to the existence and non-existence of Knut Vic designs and orthogonal Knut Vic designs, *J. Combin. Theory, Ser A*, **22**(3) (1977), 331–337.
8. A. Hedayat and W. T. Federer, On the non-existence of Knut Vic designs for all even orders, *Ann. Statist.*, **3** (1975), 445–447.
9. D. Jungnickel and G. Grams, Maximal difference matrices of order ≤ 10, *Discr. Math.*, **58**(2) (1986), 199–203.
10. T. G. Ostrom, Replaceable nets, net collineations, and net extensions, *Can. J. Math.*, **18** (1966), 666–672.

Received 18 December 1989 and accepted in revised form 8 July 1991

ANTHONY B. EVANS
Department of Mathematics and Statistics,
Wright State University,
Dayton, Ohio 45435, U.S.A.